REMARKS/ARGUMENTS

In the Office Action of January 27, 2005, Claims 1, 10, 13, 16, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,202,150 issued to Young et al. ("Young et al.") in view of Dam et al., "Cryptography's Role in Securing the Information Society"; Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Young et al. and Dam et al., and further in view of Richard Stevens (TCP/IP, illustrated, Vol. 1) ("Stevens"); and Claims 6-7 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Young et al. and Dam et al., and further in view of U.S. Patent No. 5,799,086 issued to Sudia ("Sudia").

1. Rejection of Claims 1-3, 5, 8-14, and 16-25 under 35 U.S.C. 103(a)

Amended Claim 1 claims "providing said software key to an escrow holder who is under instructions to provide said software key to said licensee upon satisfaction of a release condition, wherein said software key is otherwise unavailable to said licensee at any time."

Each of the references, including Dam et al., is directed to wiretapping of encrypted communications between private parties by law enforcement agencies. In order for the law enforcement agencies to effectively wiretap such communications, they need access to a decryption key. To gain access to the decryption key, a key escrow arrangement is provided for the law enforcement agencies. The intended recipients of the encrypted communications, however, do not need to receive the decryption key from the escrow

agent since they already have it. For example, as described in Young et al., the decryption key is the recipient's private key. See, Col. 1, lines 16-54. Therefore, the intended recipient of the encrypted communication is always in possession of the decryption key, and only the intended recipient is meant to be able to decrypt the encrypted communication.

Therefore, Young et al. does not teach "providing said software key to an escrow holder who is under instructions to provide said software key to said licensee upon satisfaction of a release condition, wherein said software key is otherwise unavailable to said licensee at any time."

To teach this element of Claim 1, the Final Office Action relies on Dam et al., and in particular, p. 12-13 in its section 5.3.

However, such reliance is incorrect, because the intended recipient, even in Dam et al., must have access to the decryption key at all times in order for the recipient to decrypt the encrypted communication. An encrypted communication system where the intended recipient cannot decrypt the encrypted message defeats the purpose of such secure communications, and makes absolutely no sense.

Reading the cited Dam et al. text, it is clear that what is meant is users never have access to the keys from the escrow agents, only law enforcement agencies acting under court order have such access. This is not meant to mean that users do not otherwise have

access to the keys, because such an interpretation would mean that they could not read the encrypted messages sent to them, and such an interpretation makes absolutely no sense.

Further, the cited text in Dam et al. indicates that the escrow agents do not even keep the user keys in escrow. They keep the communications encrypted by a session key in escrow, along with the relevant session key encrypted with the public key of the DRC. When the law enforcement agency provides a valid court order to the DRC, it receives the session key back to decrypt the specific communication.

Again, however, this does not mean that the intended recipient of the communication does not have the session key. As is well known, session keys are shared secrets between the two communicating parties. When a session key is required to decrypt an encrypted communication, the party transmitting the encrypted communication also transmits the session key (encrypted with the intended recipient's public key) to the intended recipient. The intended recipient then decrypts the encrypted session key using his/her private key, and then decrypts the encrypted message using the decrypted session key.

Therefore, it is clear that Dam et al. does not teach "providing said software key to an escrow holder who is under instructions to provide said software key to said licensee upon satisfaction of a release condition, wherein said software key is otherwise unavailable to said licensee at any time," for essentially the same reasons as discussed in reference to Young et al.

Further, as previously explained in their prior communication, applicants' source code escrow application is very different than that of the wiretapping situation described in each of the cited references. First of all, in applicants' application, the intended recipient of the encrypted source code never has access to its decryption key unless he/she receives it from the escrow agent. In this case, if the intended recipient were to already have the decryption key, it would defeat the purpose of applicants' invention.

In contrast, in the wiretapping case, the intended recipient of the encrypted message always has access to its decryption key. To have it otherwise, would defeat the purpose of its application. It is the law enforcement agency that doesn't have access to the decryption key unless it receives it from the escrow agent. This is because the law enforcement agency is not the intended recipient of the encrypted communication. Obviously, if the transmitting party wanted to provide access to the communication to the law enforcement agency, they could do so without encrypting it. The purpose of the wiretap is for the law enforcement agency to gain access to their communication without their permission or knowledge.

Further, applicants' application involves source code of a computer program, not communications or text messages. Law enforcement agencies presumably have no interest in performing wiretaps on source code transmissions, and there is no teaching or suggestion of such activity in the cited references.

To further emphasize the differences between applicants' application and the wiretapping application addressed in each of the cited references, the claims have been amended so that the recipient is a licensee of the binary executable code of the program, which clearly none of the parties receiving encrypted communications in the cited references are.

Accordingly, Claim 1 is believed to be patentable under 35 U.S.C. 103(a) over Young et al in view of Dam et al. for the foregoing reasons, as well as any other reasons stated in applicants' prior communications..

Claims 2-3, 5 and 8-9 are also believed to be patentable under 35 U.S.C. 103(a) over Younger et al. in view of Dam et al., since they depend from Claim 1, and as such, are believed to be patentable for at least the same reasons as stated in reference to Claim 1, as well as any other reasons stated in applicants' prior communications.

Amended Claim 10 is also believed to be patentable under 35 U.S.C. 103(a) over Younger et al. in view of Dam et al. for essentially the same reasons as stated in reference to Claim 1.

Claims 11 and 12 are also believed to be patentable under 35 U.S.C. 103(a) over Younger et al. in view of Dam et al. since they depend from Claim 10, and as such, are believed to be patentable for at least the same reasons as stated in reference to Claim 10, as well as, any other reasons stated in applicants' prior communications.

Amended Claim 13 is also believed to be patentable under 35 U.S.C. 103(a) over Younger et al. in view of Dam et al. for essentially the same reasons as stated in reference to Claim 1.

Claims 14 and 15 are also believed to be patentable under 35 U.S.C. 103(a) over Younger et al. in view of Dam et al. since they depend from Claim 13, and as such, are believed to be patentable for at least the same reasons as stated in reference to Claim 13, as well as any other reasons stated in applicants' prior communications.

Amended Claim 16 is also believed to be patentable under 35 U.S.C. 103(a) over Younger et al. in view of Dam et al. for essentially the same reasons as stated in reference to Claim 1.

Claim 18 is also believed to be patentable under 35 U.S.C. 103(a) over Younger et al. in view of Dam et al. since it depends from Claim 16, and as such, is believed to be patentable for at least the same reasons as stated in reference to Claim 16, as well as any other reasons stated in applicants' prior communications.

Amended Claim 21 is also believed to be patentable under 35 U.S.C. 103(a) over Younger et al. in view of Dam et al. for essentially the same reasons as stated in reference to Claim 1.

Claim 23 is also believed to be patentable under 35 U.S.C. 103(a) over Younger et al. in view of Dam et al. since it depends from Claim 21, and as such, is believed to be patentable for at least the same reasons as stated in reference to Claim 21, as well as any other reasons stated in applicants' prior communications.

2. Rejection of Claim 4 under 35 U.S.C. 103(a)

Stevens is only used in the Final Office Action to show the common known use of transferring files over the Internet using the file transfer protocol (FTP). There is no contention in the Final Office Action that Stevens teaches or suggests any of the limitations of Claim 1, and it is believed that there is no such teaching or suggestion in Stevens regarding the elements of Claim 1 that are neither taught nor suggested by Young et al. or Dam et al.

Accordingly, Claim 4 is believed to be patentable under 35 U.S.C. 103(a) since it depends from Claim 1, and as such, is believed to be patentable for at least the same reasons as stated in reference to Claim 1, as well as any other reasons stated in applicants' prior communications.

3. Rejection of Claims 6-7 and 15 under 35 U.S.C. 103(a)

Sudia is only used in the Final Office Action to show the common known use of sending information via email. There is no contention in the Final Office Action that Sudia

teaches or suggests any of the limitations of Claim 1 or Claim 13, and it is believed that there is no such teaching or suggestion in Sudia regarding the elements of Claim 1 or Claim 13 that are neither taught nor suggested by Young et al. or Dam et al.

Accordingly, Claims 6-7 are believed to be patentable under 35 U.S.C. 103(a) since they depend from Claim 1, and as such, are believed to be patentable for at least the same reasons as stated in reference to Claim 1, as well as any other reasons stated in applicants' prior communications.

Claim 15 is also believed to be patentable under 35 U.S.C. 103(a) since it depends from Claim 13, and as such, is believed to be patentable for at least the same reasons as stated in reference to Claim 13, and further since neither Young et al., Dam et al. nor Sudia, alone or in combination, teach or suggest all of the limitations of Claim 15, including its base claim and intervening claim.

Claims 1-16, 18, 21, and 23 are pending in the application. Reconsideration of the rejected pending claims is respectfully requested, and an early notice of their allowance earnestly solicited.

Respectfully submitted,

Dated: March 24, 2005

Victor H. Okumoto
Registration No. 35,973
Office Phone: (510) 792-1112